invis Server Datensicherung

Basierend auf unserer Empfehlung eine invis-Server Installation unter Nutzung von Logical-Volume-Management durchzuführen haben wir ein eigenes Datensicherungswerkzeug entwickelt, welches Datensicherung durch Kombination von LV-Snapshots und „***rdiff-backup***“ durchführt.

Als Sicherungsziele kommen wahlweise oder in Kombination externe USB bzw. eSATA Festplatten und ein gesonderter Sicherungsserver in Frage.

Sicherungsserver können von ***rdiff-backup*** direkt via „rsync over SSH“ oder SMB-Freigaben angesprochen werden. Bei der Nutzung von SMB-Freigaben gehen leider die Besitz- und Zugriffsrechte der gesicherten Dateien verloren.

Beim Einsatz externer Festplatten nutzen wir die Möglichkeiten der UDEV-Hardware Verwaltung unter Linux. Die Sicherungsplatten werden dem Server bekannt gemacht und er startet die Datensicherung automatisch, wenn „genau diese“ Festplatten mit dem Server verbunden werden. Andere Festplatten lösen keine Sicherung aus. Wichtig zu wissen, ist dass das Verbinden der Festplatte der auslösende Moment ist.

Achtung:*Die Festplatte mit dem Server verbunden zu lassen sorgt* ***nicht*** *für kontinuierlich Datensicherungen.*

Achtung: *Vor dem Gesetz gilt eine Datensicherung nur dann als Datensicherung, wenn die Sicherungen* ***räumlich getrennt*** *von den originalen Daten aufbewahrt werden. Dabei meint „räumlich getrennt“ mindestens einen anderen Brandabschnitt. D.h. Gesicherte Daten müssen durch mindestens eine Brandschutzwand und Brandschutztür von den Originaldaten getrennt sein. Ein Tresor mit Brandschutzfunktion erfüllt diese Forderung ebenfalls.*

Weiterhin fordert der Gesetzgeber von Bilanz-pflichtigen Unternehmen eine tägliche Datensicherung. Dies bedeutet für die Sicherung auf externe Festplatten, dass Sie mindestens 2 Platten im Wechsel nutzen sollten, so dass eine immer an einem gesicherten Aufbewahrungsort liegt.

Installation und Konfiguration

Die Installation ist denkbar einfach. Installieren Sie zunächst das Software-Paket „invis-rdbu“, unabhängig davon, ob Sie auf externe Platten oder einen Sicherungsserver sichern wollen.

```
linux:~ # zypper in invis-rdbu
```

Einrichten der Datensicherung auf externe Festplatten

Legen sie auf einer externen Festplatte eine einzige Partition an und formatieren Sie diese mit einem „ext3“ oder „ext4“ Dateisystem. Trennen und verbinden Sie die Festplatte nach der Formatierung neu mit Ihrem Server. Warten Sie ein paar Sekunden.

Registrieren der Sicherungsfestplatte

Während der erwähnten wenigen Sekunden Wartezeit können Sie dem Server bei der Hardware-Erkennung zuschauen:

```
linux:~ udevadm monitor
monitor will print the received events for:
UDEV - the event which udev sends out after rule processing
KERNEL - the kernel uevent
...
UDEV  [84592.431934] add
/devices/pci0000:00/0000:00:14.0/usb1/1-2/1-2:1.0/host4/target4:0:0/4:0:0:0/
block/sdc (block)
UDEV  [84592.462554] add
/devices/pci0000:00/0000:00:14.0/usb1/1-2/1-2:1.0/host4/target4:0:0/4:0:0:0/
block/sdc/sdc1 (block)
```

Wenn sich auf dem Bildschirm nichts mehr tut, ist die Erkennung abgeschlossen. Beenden ***udevadm*** mit der Tastenkombination STRG+C.

Führen Sie jetzt das Script ***udbadddisk*** aus.

```
linux:~ udbadddisk
Gefundene Festplatte: sdc
Gefundene Partition: sdc1

Gefundenes Merkmal Partitionsgröße: 3907027120
Gefundenes Merkmal Seriennummer: FDC0FD20EF00000FD0FCC4F2FFFFFF
Datensicherungsplatte hinzugefügt
```

Das Script sollte Ihnen zunächst die Bezeichnung der Festplatte (sdX) und der darauf angelegten Partition (sdX1) anzeigen. Durchsucht werden die letzten 3 Stunden des Systemjournals auf entsprechende Hotplug-Events. Wird keine geeignete Festplatte gefunden, bricht das Script ab.

Ist eine Sicherungsplatte schon länger als 3 Stunden mit dem Server verbunden und Sie kennen den Namen der darauf eingerichteten Sicherungspartition, können Sie diese Partition auch als Aufrufparameter angeben:

```
linux:~ udbadddisk sdc1
Gefundene Festplatte: sdc
Gefundene Partition: sdc1

Gefundenes Merkmal Partitionsgröße: 3907027120
Gefundenes Merkmal Seriennummer: FDC0FD20EF00000FD0FCC4F2FFFFFF
Datensicherungsplatte hinzugefügt
```

Das Script ***udbadddisk*** ermittelt Informationen zur eindeutigen Identifikation der Festplatte und generiert daraus eine UDEV-Regel in der Datei:

```
/etc/udev/rules.d/80-backupdisk.rules
```

Hier die im oben gezeigten Beispiel entstandene UDEV-Regel:

```
SUBSYSTEMS=="usb", KERNEL=="sd*",
ATTRS{serial}=="FDC0FD20EF00000FD0FCC4F2FFFFFF", ATTR{size}=="3907027120",
SYMLINK+="backup", RUN+="/usr/bin/udbdiskplugged"
```

Sie besagt, wenn ein Gerät des Typs „sd“ am USB-Bus mit der Seriennummer „FDC0FD20EF00000FD0FCC4F2FFFFFF“ und der genannten Partitionsgröße erkannt wird, soll unter „/dev“ ein Symlink unter dem Namen „backup“ angelegt werden, der auf das gefundene Gerät verweist (/dev/sdX1). Danach soll das Script ***udbdiskplugged*** ausgeführt werden.

Sicherung konfigurieren

Sind alle Sicherungsfestplatten vorbereitet, kann die Sicherung selbst konfiguriert werden. Dies erledigt das Script ***udbconf***

Zur Verwendung von ***udbconf*** müssen Sie sich im Klaren sein, was Sie sichern wollen.

Wie eingangs bereits erläutert, setzt „invis-rdbu“ die Verwendung von Logical-Volume-Management zwingend voraus. Zur Konfiguration der Datensicherung benötigen Sie den Namen der Volume-Group und der darauf liegenden zu sichernden Volumes. Sichern sollten Sie grundsätzlich alle logischen Volumes des Servers, nur dann ist es möglich eine vollständige Server-Installation aus der Sicherung wiederherzustellen. Wenn Sie bei der Partitionierung der Server-Festplatten gemäß unserem Beispiel hier im **Wiki** vorgegangen sind, sind das die Volumes:

- **root**
- **home**
- **srv**
- **var**

Sollten Sie die Namen der Volume-Group und der darin liegenden Volumes nicht mehr wissen, können Sie sie mit folgenden Kommandos anzeigen:

Volume-Group scannen:

```
linux:~ # vgscan -v
```

Logical Volumes scannen:

```
linux:~ # lvscan -v
```

Weiterhin müssen Sie die Größe des zu verwendenden Snapshot-Volumes festlegen. Die maximal mögliche Größe zeigt ***udbconf*** an. Normalerweise sollte eine Snapshot-Volume-Größe von 20GB ausreichen.

udbconf starten:

```
linux:~ # udbconf
Datensicherung udrdbu wird konfiguriert
```

```
Geben Sie bitte den Namen der Volume-Group ein, in der sich die zu
sichernden logical Volumes befinden: system
Geben Sie bitte die Namen der zu sichernden logical Volumes ein. z.B. srv
(Mehrere Volume-Namen durch Leerzeichen trennen.): root srv home var
Geben Sie bitte den vollständigen Namen des zuständigen Administrators ein:
Stefan Schäfer
Geben Sie bitte die Mail-Adresse an, an die Datensicherungsmeldungen
geschickt werden sollen: info@local-net.loc
Geben Sie bitte die Mail-Adresse an, die als Absender verwendet werden
sollen: backup@local-net.loc
Geben Sie bitte die Größe des Snapshotvolumes an. Die Größe muss größer als
die größte zu sichernde Datei und kleiner als 357,50 GiB sein. (Angabe xxG):
20G
Konfiguration abgeschlossen
```

Hier die resultierende Konfigurationsdatei:

```
# Konfigurationsdatei fuer invis-rdbudisk
# (c) 2010-2016 Stefan Schaefer - invis-server.org

# Zielhost
targetHost:localhost
targetDirUDEV:/mnt/udevsync/rdbackups

# LVM Daten
volumeGroup:system
# Mehrere Volume Namen durch Leerzeichen trennen
sourceVolume:root srv home var
# Groeße des Snapshots -> Achtung bei Images von virtuellen Maschinen,
# hier muessen die Images in den Snapshot passen.
snapshotSize:20G

# Admin
adminitrator:Stefan Schäfer

# Mail-Absender und -Empfaenger
mailTo:info@local-net.loc
mailFrom:backup@local-net.loc
# nur im Fehlerfall oder immer Mails versenden.
# Werte: always, failure
mailWhen:failure

#Backupuser
buServerUser:root
```

Grundsätzlich versucht „invis-rdbu“ Emails zu versenden, die generell über die Durchführung der Datensicherung informieren, oder nur Fehler melden. Voreingestellt ist das Versenden von Mails im Fehlerfall. Diese Einstellung kann manuell in der automatisch erzeugten Konfigurationsdatei

```
/etc/invis/rdbudisk.conf
```

angepasst werden.

Das Web-Portal des invis-Servers ist ebenfalls in der Lage über Erfolg oder Misserfolg der Datensicherung zu informieren. Diese Funktion muss zunächst in der Konfiguration des invis-Portals frei geschaltet werden. Öffnen Sie für diesen Zweck die Datei:

```
/etc/invis/portal/config.php
```

und befreien Sie die Zeile:

```
// Bitte folgende Zeile von den Kommentarzeichen befreien, wenn udevsync zur
Datensicherung verwendet wird.
$STATUS_BACKUP_TIMER = 3;
```

von den führenden Kommentarzeichen (Doppel-Slash '/'). In dieser Zeile können Sie auch den gewünschten Sicherungszyklus vorgeben. Das Portal wird dann deutlich darauf hinweisen, wenn eine Sicherung nicht wie geplant durchgeführt wird.

Die Anzeige erfolgt im Portal auf der Seite „Status“.

Testen

Vor allem, wenn Sie die Einrichtung remote vornehmen ist es wichtig einen Test der Sicherung durchführen zu können, ohne, dass Ihnen helfende Hände zur Seite stehen. Dazu müssen Sie einen „uevent“ triggern, damit die neue UDEV Erkennungsregel angewendet wird:

```
linux:~ echo change > /sys/block/sdX/uevent
```

Einrichtung der Datensicherung auf einen Sicherungsserver

Der Sicherungsserver selbst benötigt einfach nur eine Linux-Installation mit genügend Festplattenplatz. Auf ihm muss der SSH-Dienst laufen und ***rdiff-backup*** installiert sein.

SSH vorbereiten

Damit die Sicherung über SSH erfolgen kann, muss sich der Benutzer „root“ des Quell-Servers ohne Passwort per SSH am Sicherungsserver anmelden können. Es ist nicht notwendig, dass auch auf dem Sicherungsserver das Konto des Benutzers „root“ verwendet wird. Es genügt dort ein Benutzerkonto, welches Schreibrecht im Zielverzeichnis der Datensicherung hat.

Die passwortlose Anmeldung gelingt, wenn die Authentifizierung am Sicherungsserver mit einem Schlüssel erfolgt. Dieser Schlüssel kann auf dem Quellserver (angemeldet als Benutzer „root“) einfach generiert werden:

```
Generating public/private rsa key pair.
Enter file in which to save the key (/root.sshid_rsa):
Enter passphrase (empty for no passphrase):
```

```
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
fb:8b:20:3d:97:25:09:e7:ef:fe:63:d1:b3:49:1f:e0 [MD5] root@server
The key's randomart image is:
+--[ RSA 2048]----+
|                 |
|                 |
|      . .        |
|       + .   .   |
|        S . ...  |
|     .   *  .E+. |
|    . + + .  o =.|
|     . + +  o o .|
|        ..=+..   |
+--[MD5]----------+
```

Kopieren Sie dann (auf sicherem Weg) den öffentlichen Teil (public key) des erzeugten Schlüsselpaares in des Home-Verzeichnis des Backup-Benutzerkontos auf dem Sicherungsserver:

```
linux:~ # scp .ssh/id_rsa.pub backup@backupserver:~
```

Melden Sie sich jetzt am Backupserver mit diesem Konto an und hängen Sie den Schlüssel an die Datei „authorized_keys“ in dessen Homeverzeichnis an:

```
backup@backupserver:~ # cat id_sa.pub >> .ssh/authorized_keys
```

Damit der SSH-Dienst des Backup-Servers die Anmeldung per Schlüssel akzeptiert müssen in der Konfigurationsdatei des SSH-Servers

```
/etc/ssh/sshd_config
```

folgende Einträge vorhanden sein:

```
...
PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and
.ssh/authorized_keys2
# but this is overridden so installations will only check
.ssh/authorized_keys
AuthorizedKeysFile      .ssh/authorized_keys
...
```

Ist das der Fall, können sie einen Login-Versuch unternehmen:

```
linux:~ ssh backup@backupserver
```

Gelingt dies ohne Passwortabfrage, ist die Vorbereitung abgeschlossen.

Sicherung einrichten

Das Einrichten einer Sicherung auf einen externen Server läuft analog zur Sicherung auf externe Festplatten ab. Es existiert mit ***rdbunetconf***auch hier ein Script, welches die Konfigurationsdatei zur Sicherung generiert. Es ist einfach ohne weitere Optionen aufzurufen:

```
invis:~ # rdbunetconf
```

Im Verlauf des Scripts wird gefragt, ob die Sicherung via SSH oder auf eine einzuhängende SMB-Freigabe erfolgen soll. Wir empfehlen ganz eindeutig die SSH-Methode zu bevorzugen. Die SMB-Methode ist eher eine Notlösung, beispielsweise zur Sicherung auf ein NAS System welches lediglich via SMB nutzbar ist. Dabei kommt es allerdings immer wieder zu Problemen, beispielsweise wegen maximaler Pfadlängen, unterschiedlichen Zeichensätzen oder auch der Konsistenz von Zugriffs- und Besitzrechten.

Durchführung und Kontrolle

Sicherung auf Backupserver

Wird auf einen Server gesichert, müssen Sie sich um die Durchführung der Datensicherung keine Gedanken machen, sie erfolgt automatisch, zeitgesteuert.

Sicherung auf externe Festplatten

Wird auf externe Festplatten, ist das Verbinden der Platte mit dem Server das auslösende Ereignis. Das bedeutet auch, dass Sie die Sicherungsfestplatte nach erfolgter Sicherung wieder vom Server trennen müssen.

Achtung*: Lassen Sie eine Sicherungsfestplatte am Server angeschlossen, werden* ***nicht*** *automatisch regelmäßige Datensicherungen durchgeführt.*

Die ideale Vorgehensweise ist eine abwechselnde Datensicherung auf zwei Festplatten. D.h. Eine der Festplatten ist mit dem Server verbunden, während die zweite an einem „sicheren“ Ort aufbewahrt wird. Tauschen Sie idealerweise zu einem Zeitpunkt an dem wenig oder nicht auf dem Server gearbeitet wird die Festplatten aus.

Sie können die verbundene Festplatte dabei einfach ohne weitere Vorbereitung vom Server trennen, die logische Trennung wird nach erfolgter Sicherung bereits vom Sicherungsprogramm vorgenommen.

Daten wiederherstellen

… work in progress …

Aufräumen

Wir haben festgestellt, dass gerade bei der Verwendung von externen Sicherungsfestplatten immer wieder Probleme auftreten, beispielsweise, weil Festplatten versehentlich getrennt werden noch während eine Sicherung läuft. Um derartiges zu vermeiden zeigt das invis-Portal inzwischen wesentlich deutlicher an, dass eine Sicherung aktiv ist. Dies setzt natürlich die Nutzung des invis-Portals voraus….

Um nach einem Abbruch einer Sicherung verwaiste Mounts oder Snapshot-Volumes wieder los zu werden läuft per Cornjob alle 3 Minuten das Script ***dasimonitor***. Das Script ist auch die Quelle der Informationen die im invis-Portal angezeigt werden.

Kopano Datensicherung

Die Groupware Kopano bringt ein eigenes Brick-Level Backup-System mit. invis-Server sind so eingerichtet, dass sie täglich abwechselnd einmal die komplette Kopano-Datenbank in Form eines Dumps sichern und einmal das Bricklevel-Backup durchführen. Dabei dient die gesicherte Datenbank als Disaster-Recovery, also dem Wiederherstellen der gesamten Datenbank im Falle eines Crashs und das Bricklevel-Backup dem Wiederherstellen einzelner Elemente, beispielsweise wenn diese versehentlich gelöscht wurden.

Ziel beider Sicherungen ist das Verzeichnis:

```
/srv/shares/sicherungen
```

Wiederherstellung einzelner Elemente aus dem Brick-Level Backup

Das benötigte Werkzeug ist ***kopan-backup***, es bietet verschiedene Möglichkeiten Elemente eines geicherten Kopano-Stores wiederherzustellen. Beginnen wir damit uns den Inhalt der Sicherung anzeigen zu lassen. Wechseln Sie dazu ins Verzeichnis in dem die gesicherten Stores liegen:

```
/srv/shares/archiv/sicherungen/kopanostores
```

Der folgende Befehl gibt den gesamten Inhalt eines gesicherten Benutzer-Stores aus:

```
invis:/srv/shares/archiv/sicherungen/kopanostores # kopano-backup --index
username
```

Im Beispiel steht „username“ sowohl für den Namen des Sicherungverzeichnisses eines Benutzers, als auch für den aktiven Benutzer in dessen Store ein oder mehrere Elemente wiederhergestellt werden sollen.

Mit der Option **`-u username2`** können Elemente auch in einen anderen aktiven Store wiederhergestellt werden.

Um die Ausgabe einzugrenzen, ist ***grep*** ein geeignetes Werkzeug:

```
invis:/srv/shares/archiv/sicherungen/kopanostores # kopano-backup --index
username | grep Posteingang
```

Die Ausgabe der Informationen erfolgt tabellarisch, Spaltentrenner ist das Komma. Nachfolgend der Aufbau der Zeilen:

```
Eindeutige ID,Ordner,Datum Uhrzeit,Betreff oder Property
```

Anhand der ID können einzelne Elemente wiederhergestellt werden. Suchen Sie zunächst wie oben gezeigt das wiederherzustellende Element, beispielsweise anhand des Betreffs oder des Datums eines Elementes. Nutzen Sie jetzt die ID des gesuchten Elements um es wiederherzustellen:

Wiederherstellen eines einzelnen Elementes

```
/srv/shares/archiv/sicherungen/kopanostores # kopano-backup --restore
username --sourcekey DFD123BE9FD84F7AB08E00DD959F2730080100000000
```

Wiederherstellen aller Elemente eines Ordners

```
/srv/shares/archiv/sicherungen/kopanostores # kopano-backup --restore
username -f Posteingang
```

Dabei wird im Store des Benutzers nichts überschrieben. Bereits vorhandene Elemente werden automatisch übersprungen.

Wiederherstellung der vollständigen Datenbank

Achtung*: Die Wiederherstellung der Kopano-Datenbank sollten Sie nur durchführen, wenn die vorhandene Datenbank irreparabel beschädigt ist. Die vorhandene Datenbank wird bei der Wiederherstellung vollständig überschrieben.*

Es gibt zwei mögliche Vorgehensweisen. Die Sicherung liegt gezippt vor. Sie können die Datei, wenn gewünscht zunächst entzippen und dann wiederherstellen, oder Sie führen beide Schritte in einem durch.

2 Schritte

```
invis:~ # gunzip gunzip
/srv/shares/archiv/sicherungen/vollsicherungen/datenbanksicherungen/20171003
/kopano.invis.20171003.gz
invis:~ # mysql -u root -p kopano <
/srv/shares/archiv/sicherungen/vollsicherungen/datenbanksicherungen/20171003
/kopano.invis.20171003
```

1 Schritt

```
invis:~ # gunzip <
```

```
/srv/shares/archiv/sicherungen/vollsicherungen/datenbanksicherungen/20171003
/kopano.invis.20171003.gz | mysql -u root -p kopano
```